

# EL USO SEGURO DE LAS NUEVAS TECNOLOGÍAS



AYUNTAMIENTO DE SEVILLA

### PARA EMPEZAR:

Las Nuevas Tecnologías de la Información y la Comunicación (TICs) tienen muchas ventajas y ya forman parte de la vida de las nuevas generaciones. Para la mayoría de la gente joven, internet, los videojuegos o los teléfonos móviles, son un medio para relacionarse, informarse, jugar, estudiar, escuchar música. etc.

Sin embargo, por muy divertidas que sean, no son un juguete, encierran riesgos potenciales y reales para menores y jóvenes, como son: que niñas y niños vean contenidos no adecuados para su edad, el robo de datos personales, la suplantación de identidad o el ciberacoso (acoso a través de internet). Por eso es necesario enseñarles a utilizar las tecnologías digitales de un modo adecuado, estando con ellas y ellos en todo momento hasta que aprendan un modo seguro y responsable de navegar por las mismas. A veces, en la familia, se piensa que las y los menores son expertas y expertos en estas materias, lo que impide que se tomen medidas de control y seguridad y, sobre todo, que se les dé una información adecuada sobre el buen uso que deben hacer de ellas.

Para ello, las personas adultas deben estar siempre en un proceso de información y adaptación constante, debido a la rapidez con la que cambian y evolucionan estas nuevas tecnologías de la comunicación.

Hay que partir de una realidad:

Descenso en la edad de inicio en el uso de las TICs.

Posibilidad de conexión permanente.

UN SMARTPHONE (teléfono móvil inteligente) ES UN ORDENADOR DE BOSILLO.

### **ALGUNOS DATOS**

Aunque todas y todos conocemos la magnitud del uso que la juventud hace de Internet, redes sociales, aplicaciones de mensajería instantánea (principalmente WhatsApp) y de la influencia que tiene sobre sus vidas, así como los riesgos potenciales que ello implica, vamos a concretarlo sobre datos estadísticos:

España tiene una población on line de 23 millones de personas.

El 89% de las y los españoles mayores de 13 años posee un teléfono móvil.

El principal dispositivo para acceder a internet es a través de los teléfonos móviles (100%), seguido de los ordenadores (portátiles o de sobremesa) y las tablets.

Entre las y los jóvenes de 18 a 24 años mirar el móvil es casi una necesidad, el 88% lo mira antes de cinco minutos después de haberse levantado.

9 de cada 10 personas en España usa WhatsApp.

Las aplicaciones gratuitas son usadas de forma mayoritaria para conectarse desde los teléfonos móviles.

Las personas entre 16 y 29 años, configuran el grupo poblacional más expuesto a sufrir ciberacoso.

Entre las chicas y los chicos de 13 a 14 años el 15% ha chateado con personas desconocidas.

El 13,7% de las chicas y los chicos de 13 a 14 años ha recibido mensajes de contenido sexual.

El 10,3% de adolescentes de 15 a 19 años ha encontrado contenidos explícitamente violentos o sexuales.

El 7,4% de las chicas de 15 a 29 años reconoce haber sido objeto de acoso on line, reduciéndose este porcentaje en el caso de los chicos hasta un 2,1%.



### También tenemos que conocer para qué usan las y los jóvenes las TICs. Las prácticas sociales "virtuales" más habituales son:

- Compartir contenidos como fotografías, vídeos, webs, textos, músicas o noticias.
- Enviar mensajes privados.
- Participar en juegos on line.
- Comentar el contenido compartido por otras personas.
- Publicar eventos.
- Hablar en tiempo real con otras personas mediante chats u otros.
- Crear grupos exclusivos para determinados contenidos.
- Publicar comentarios en el perfil o espacio personal de otras personas usuarias.

Los riesgos en la red más relevantes para menores y adolescentes (según la Agencia de Calidad de Internet) son:



### RIESGOS PERSONALES

conductas de acoso.

Hay quienes aprovechando el anonimato que permite Internet, la inmediatez y el gran número de personas destinatarias a las que llega casi de forma instantánea, llevan a cabo c o m p o r t a m i e n t o s abusivos y/o violentos, especialmente con niñas y chicas jóvenes, a través principalmente de redes sociales.

Algunas de estas conductas pueden ser las siguientes:

### Ciberacoso o ciberbullying

Menores y adolescentes pueden ser víctimas de ciberbullying cuando a través de Internet, teléfonos móviles, consolas de juegos u otras tecnologías telemáticas, son objeto de amenazas, humillaciones, hostigamiento, etc., por otra persona que también es menor de edad y que conocen en su vida "real".

#### Acoso sexual o grooming

También pueden ser objeto de acoso sexual o grooming cuando una persona mayor de edad intenta ganarse su confianza a través de la Red para conseguir que le faciliten datos personales y de contacto, imágenes en las que aparezcan en ropa interior, de baño o semidesnuda/o, que posen ante la webcam con posturas "provocativas" o "eróticas" o en definitiva para concertar encuentros sexuales en la vida "real".

#### Sextorsión o ciberchantaje

Esta conducta está relacionada con la práctica del sexting, que consiste en enviar a otras personas, fotos y/o vídeos de carácter sexual.

No necesariamente tienen que se relaciones sexuales explícitas, pueden ser fotos en ropa interior, en pose "provocativa", donde se aparezca semidesnuda/o, mensajes "calientes", etc., que ha realizado la propia persona que lo remite u otra con su consentimiento.

Por lo tanto, la práctica del sexting en sí misma no es delictiva, aunque sí peligrosa, ya que una vez que hemos enviado esa información, no se tiene ningún control sobre ella, además del riesgo que existe de pérdida o robo del teléfono móvil, con toda la información que contiene.

En este sentido, debemos informar e intentar hacer ver a nuestras hijas y nuestros hijos, sobre lo arriesgado de esta práctica y las consecuencias negativas que puede tener, una de ellas, la sextorsion o ciberchantaje, que se produce cuando una persona utiliza los contenidos sexuales a los que ya tiene acceso y amenaza con publicarlos si la persona a la que chantajea no le envía nuevas imágenes o vídeos, no consiente tener contactos sexuales, no continúa con la relación de pareja, etc.

### Revengeporn, pornovenganza o porno vengativo

Esta conducta consiste en el uso y la difusión masiva a través de las redes sociales y/o plataformas de mensajería instantánea como WhatsApp, de imágenes y/o vídeos de carácter sexual, con la finalidad de causar daño a la persona cuyas imágenes íntimas se publican y que no ha consentido el uso público de las mismas.

Normalmente son conductas realizadas por ex parejas como forma de venganza por haber dejado la relación y las víctimas son principalmente mujeres. Son estrategias humillantes que afectan a la privacidad e intimidad de las víctimas, además del daño que supone a su imagen pública.

Una cultura machista donde el ejercicio de la sexualidad por las mujeres se percibe socialmente de manera muy diferente al equivalente por parte de los hombres, unida a la normalización de la grabación e intercambio de imágenes íntimas entre parejas, son el caldo de cultivo para que la pornovenganza esté cobrándose cada vez más víctimas y constituyendo una forma creciente de violencia de género sexual digital (www.pantallasamigas.net).

Además de quienes realizan directamente estas conductas, debemos tomar conciencia de que en muchos casos estas acciones y el daño que producen, se ve incrementado por todas aquellas personas que "siguen la cadena" y que, por lo tanto, se convierten en cómplices, lo hagan de forma consciente o no. En este sentido:

Debemos informar a nuestras/os menores, de la responsabilidad penal en que pueden incurrir. Debemos procurar que tomen conciencia del daño que están causando a la persona cuya imagen están difundiendo.

Debemos trasmitirles el mensaje de que esa persona es la víctima, no la responsable, aunque diera su consentimiento para la grabación de las imágenes, basado en una relación de confianza, como es una relación de pareja o en el ejercicio de su libertad de decisión, pero que esto no da derecho a la otra persona a su difusión y menos como una forma de venganza.

### La difusión supone mayor agravio que sólo la grabación

Las descritas pueden conductas conllevar responsabilidad penal, puesto que a través de ellas se realizan delitos recogidos en nuestro Código Penal, como pueden se amenazas falsas acusaciones, suplantación de identidad, usurpación de datos calumnias, personales. injurias, coacciones. pornografía infantil, abusos sexuales, contra el honor,..., por lo tanto, debemos hacer ver a nuestras y nuestros jóvenes, que la participación en estas conductas en el grado que sea, como autoras/es, como cómplices, "jaleando", "picando", no es un juego, no sólo porque produce daño a la persona a la que se dirige, también porque puede ser causa de responsabilidad penal.

### Amenazas a la privacidad

Puede producirse cuando se proporciona a través de Internet, información sobre su vida o imágenes, para poder acceder a espacios comunes

(plataformas, redes sociales,...), para utilización gratuita de servicios o como forma de relacionarse y comunicarse con amigas/os. Muchas webs, blogs, Apps (que son las más usadas) solicitan datos para un uso fraudulento de los mismos. Esta exposición de la vida privada en la Red también está muy relacionada con las conductas de acoso descritas anteriormente, por ello debemos explicarles e informar sobre los riesgos que conlleva el "colgar" información y/o imágenes en la Red, es muy importante promover "la cultura de la privacidad":

Enseñarles que nunca deben enviar, a personas desconocidas. datos personales las/los aue identifiquen (nombre, apellidos, edad, teléfono, dirección de casa o del cole, contraseñas,...) y que tengan la misma precaución con la información familiares. amistades personal de SUS conocidas/os. Facilitar el nº de teléfono móvil puede hacer que la línea quede suscrita a un servicio SMS Premium, con el consiguiente perjuicio económico. Se recomienda deshabilitar esta opción contactando con su compañía telefónica.

Explicarles que eviten publicar fotos o conectar la webcam con personas desconocidas, además de taparla cuando no se utilice, incluso aunque el ordenador esté apagado.

(www.cuidadoconlawebcam.com)

Hablarles sobre el respeto a la intimidad cuando se suben y/o etiquetan fotos en las que aparecen otras personas. Es importante advertirles que siempre debemos contar con su consentimiento antes de hacerlo.

Decirles que no concierten citas con personas que hayan conocido a través de la Red.

Pedirles que cierren inmediatamente cualquier página, chat o mensaje que les haga sentirse incómodas/os.

ALGUNOS INDICADORES QUE PUEDEN HACERNOS SOSPECHAR QUE NUESTRA HIJA O NUESTRO HIJO, ES VÍCTIMA DE ALGUNA DE LAS CONDUCTAS MENCIONADAS ANTERIORMENTE SON:

Cambio de hábitos: en el uso de dispositivos (móviles, tablets...) o de Internet; abandono o ausencia en actividades hasta ese momento preferidas; altibajos en los tiempos de estudio y en el rendimiento del trabajo escolar; ocultamiento especial cuando se comunica por Internet o teléfono móvil...

Cambios en el estado de ánimo: cambios de humor; momentos de tristeza, apatía o indiferencia; explosiones momentáneas de agresividad... Cambio en sus relaciones habituales: cambios en sus grupos de amistades, en ocasiones cambios radicales; repentina pobreza, ausencia de amistades y de relaciones sociales; falta de defensa o exagerada reacción ante supuestas bromas u observaciones públicas; miedo u oposición a salir de casa; excesivas reservas en la comunicación...

Cambios físicos: modificaciones en su lenguaje corporal ante la presencia de determinadas personas (hombros encorvados, cabeza gacha, falta de contacto en los ojos, etc.); pérdida y/o deterioro de pertenencias físicas sin explicaciones razonables; manifestaciones de enfermedad o dolencias frecuentes; dolores de cabeza o de estómagoq u e no ocasionan despertares nocturnos pero que impiden realizar actividades normales como el ir al centro educativo...



## RIESGOS DE CONTENIDO

acceso voluntario o involuntario, a contenidos no apropiados.



#### Acceso a contenidos no adecuados

La posibilidad de acceder a la información que Internet ofrece, viene acompañada de un riesgo que es la posibilidad de que menores y adolescentes puedan encontrar imágenes o información de contenidos inapropiados: violentos. discriminatorios. sexistas. racistas.... **Estos** contenidos pueden llegarles al acceder determinadas páginas, blogs, foros o a través de SPAM (correo electrónico "basura"). pueden encontrarse con la publicidad emergente o "pop ups", pequeñas ventanas que se abren en el navegador encima de la página web que se está viendo, que en muchas ocasiones vienen referidas a contenidos. servicios v/o informaciones inapropiadas para ellas/os, o a través de la publicidad explícita que se utiliza de forma masiva sociales las redes (Facebook, Instragram,...) o "redes de spammers" que utilizan plataformas estas para insertar contenidos inapropiados



(http://www.eldiario.es/consumoclaro/consumo\_digital/videos-porno-instagram-sexo\_0\_600190626.html).

Para evitar esto es importante instalar un buen filtro de seguridad, que es una herramienta para impedir el acceso a este tipo de contenidos, para ello se puede visitar la página www.archivospc.com. que programas gratuitos de filtrado. Además. existen buscadores específicamente diseñados para menores como son Yahoo! Kids. Ask Kids v Kids Click v algunos buscadores generales permiten filtrar determinados contenidos direcciones v inapropiadas a través de algunas opciones de configuración, son los denominados Safe Search que pueden encontrarse en Google, Yahoo, Bing... la aplicación de vídeo YouTube, también tiene la versión dedicada exclusivamente a menores: YouTube Kids.

Pero, iojo!, estos filtros, buscadores y configuraciones específicas, nunca deben sustituir la necesaria labor de supervisión que deben realizar las personas adultas.

Información abundante y de fácil acceso Internet es una fuente inmensa de información, pero ésta puede ser errónea, incompleta, inadecuada o interesada. Existen muchas webs, blogs, youtubers, instagramers,... que ofrecen un conocimiento, una

opinión, una visión, un reclamo sobre algún tema concreto, menores, adolescentes y jóvenes, asumen como "verdad absoluta", como real, sólo porque está en la Red, pero no siempre es así.

### **Algunas recomendaciones son:**

Decirles que busquen fuentes que ofrezcan credibilidad y rigor en sus informaciones u opiniones y contrastar cualquier noticia, reclamo, que encuentren en la Red. Que no se queden con la primera versión.

Animarles a saber buscar y a seleccionar los contenidos.

### Spam, virus y otros

Cuando nuestras niñas v nuestros niños adolescentes tienen cuentas de correo electrónico o acceso a redes sociales, se exponen a la posibilidad de recepción de spam que invaden el ordenador, teléfono móvil o tablet e incluso pueden bloquear sus cuentas. Además pueden ir acompañados virus, también "gusanos y troyanos", que causan problemas los dispositivos: borrando información, tomando el control del mismo, adquiriendo información sensible, etc. Estos riesgos están muy relacionados con las descargas de archivos (música, películas, juegos,...) que realizan.

Para evitar esto es importante, adoptar algunas

### MEDIDAS DE SEGURIDAD



Proteger el ordenador, tablet o móvil con un sistema antivirus y "cortafuego" (firewall) y mantenerlos actualizado. Ya existen multitud de Apps que son seguras, gratuitas y eficaces que tienen este cometido.

Utilizar los sistemas antispam del proveedor de Internet, del programa de correo electrónico o alguna App.

Instalar en el ordenador, tablet, móvil o consola algún sistema de filtro que limite el acceso a páginas de contenido inapropiado.

Utilizar contraseñas fuertes que son aquellas que reuniendo algunas características (longitudmínima, uso de mayúsculas y minúsculas, inclusión de números...) tienen menos probabilidad de que alguien las averigüe, cambiarla cada cierto tiempo, además de que no sea siempre la misma.

## RIESGOS DE ADICCIÓN.



adquirir comportamientos de dependencia al uso de Internet.

### Algunas de las características que tiene el uso de Internet, como son:

- la inmediatez
- la posibilidad de adoptar otra identidad el anonimato
- la sensación de gratificación (likes, seguidoras/es, comentarios en publicaciones...)
- la facilidad de acceso
- -la posibilidad de estar continuamente conectadas/os (bien a través de mensajería instantánea, chats, imágenes y/o vídeos) pueden llegar a provo- car situaciones de dependencia.

Podemos definir la Adicción a las Nuevas Tecnologías como la conducta obsesiva compulsiva que se desarrolla cuando usamos excesivamente aparatos tecnológicos, provocando un deterioro en los componente biológico, psicológico y social (Peláez 2009).

La adicción a la tecnología comienza cuando abusamos de los distintos aparatos electrónicos y estos nos van robando tiempo de los procesos de socialización básicos para el desarrollo personal y familiar.

Algunos indicadores que pueden hacernos sospechar que la o el menor se encuentra en esta situación son:

- Bajo aprovechamiento académico/ fracaso escolar.
- Dormirse en las clases.
- Distraerse pensando en internet, redes sociales o juegos.
- Falta de relación con amistades.
- Conducta violenta con sus compañeras/os.
- Evitación de relaciones sociales
   "persona a persona".
- Pobre destreza de comunicación verbal y escrita.
- Limitaciones en la imaginación y la creatividad.

Para intentar evitar estas conductas adictivas, lo mejor es prevenir, educando en un buen uso de las TICs. Así, con carácter general, sería importante elaborar un CÓDIGO DE USO DE INTERNET CONSENSUADO para toda la familia donde se establezca:

CÓMO, qué herramienta se puede usar: ordenador, móvil, tablet, videojuegos,...

CUÁNDO, delimitar horario y tiempos de uso.

DÓNDE, lugares en los que pueden usarse los diferentes aparatos tecnológicos: en casa, en el cole, casa de amigas/os, zonas wifi,...

PARA QUÉ se van a usar.

Plasmarlas POR ESCRITO y fijarlas en un SITIO VISIBLE.

### Y tomar también medidas concretas como, por ejemplo:

Omitir las notificaciones (sonoras y visuales) de las redes sociales en el móvil.

Reducir las 'amistades' o personas a las que seguimos en las redes para centrarnos sólo en quienes realmente nos interesen.

Restringir el uso de juegos y aplicaciones.

Fomentar el desarrollo de otras actividades lúdicas (deportes, lectura, aficones,...).

Procurar apagar el móvil durante las horas de descanso (1 de cada 3 personas nunca apaga el móvil).

Además, para saber más, puede visitarse la página www.tecnoadicciones.es

La MEDIDA más IDÓNEA para evitar los riesgos en el uso de las Nuevas Tecnologías es la PREVENCIÓN

PARA QUE LAS PERSONAS ADULTAS PUEDAN PONER EN PRÁCTICA LAS RECOMENDACIONES Y CONSEJOS MENCIONADOS, ES NECESARIO:

Estar al día sobre nuevas tecnologías, siendo conscientes de la velocidad con la que van cambiando y ofreciendo nuevas formas de comunicación e información.

Actuar como referentes y modelos para nuestras/os menores y adolescentes en relación a las TICs. Sé tú misma o tú mismo un buen ejemplo de su uso.

Fomentar la confianza y la buena relación con nuestras hijas e hijos para que tengan libertad para contarnos cualquier contratiempo que tengan en el uso de las mismas. Comentar con naturalidad y regularidad los riesgos que tiene el acceso a internet y orientar sobre las posibilidades de configuración de privacidad de las múltiples redes sociales que utilizan.

Navegar, chatear, jugar,... de vez en cuando con ellas y ellos y así conocer sus hábitos y preferencias y crear un clima de mayor confianza.

Supervisar activamente el uso que hacen de las Nuevas Tecnologías.

Procurar que los distintos dispositivos tecnológicos: ordenador, tablet, móvil y/o consola se utilicen bajo unas normas, con un objetivo concreto y bajo supervisión.

Controlar las aplicaciones que se van a descargar leyendo los permisos que se solicitan y comprobando si guardan relación con la funcionalidad de la App. Es muy importante, que la familia utilice sistemas de contraseñas que les permitan, al menos, aprobar el tipo de aplicaciones móviles que van a instalar y utilizar sus hijas e hijos.

Enseñar a utilizar las herramientas tecnológicas con criterio, haciendo un buen uso de los aspectos positivos que aportan.



Ofrecer pautas de cómo afrontar las situaciones de riesgo que puedan producirse: pedir ayuda,contarlo; bloquear a quien acosa; guardar las evidencias,...

### **VIOLENCIA DE GÉNERO Y NUEVAS TECNOLOGÍAS**

Hay que hacer una especial referencia a la violencia de género que se realiza a través del uso de las TICs (plataformas o sistemas virtuales como el correo electrónico, sistemas de mensajería, Whatsapp, redes sociales, blogs o foros, webs,...) siendo su objetivo la dominación, discriminación, el abuso de la posición de poder. Por lo tanto, la ciberviolencia de género tiene la misma finalidad que la violencia de género "real" sólo que se ejerce con otras herramientas "virtuales".

La ciberviolencia de género tiene unas características específicas debidas precisamente al entorno "digital" en la que se realiza, así tiene un carácter dinámico, veloz, de conectividad, sin necesidad de contacto físico con la víctima, con una posibilidad ilimitada de difundir de la información.

A través de la Red se ejerce violencia contra las mujeres en el ámbito de las relaciones de pareja, pero también nos encontramos con la violencia sexual, la pornografía, la explotación sexual o los matrimonios forzados.

Las mujeres jóvenes son más vulnerables al daño del ciberacoso por la desigualdad en la consideración y valoración social a la que se someten los comportamientos y las imágenes de las mujeres. En general, en cualquier ámbito donde se produzca y concretamente, en el ámbito delas relaciones de pareja.

En cuanto a la Ciberviolencia en el ámbito de una relación de pareja, hay determinadas conductas que pueden ser más fácilmente identificadas por la mujer, debido a la mayor gravedad que revisten y porque cuando se producen, normalmente, va se ha puesto punto v final a la relación: distribuir en Internet una imagen comprometida de contenido sexual (real o trucada) o datos susceptibles de perjudicar a la víctima; darla de alta en un sitio web donde puede estigmatizarse v ridiculizar a la persona: crear un perfil o espacio falso en nombre de la víctima en el que ésta comparte intimidades. realiza demandas y ofertas sexuales explícita,...; usurpar la identidad de la víctima y, en su nombre, hacer comentarios ofensivos o participaciones inoportunas en chats de tal modo que despierte reacciones adversas hacia quién en verdad es la víctima: engaño haciéndose pasar por amigas o amigos: enviar mensaies ofensivos y hostigadores a través de email. WhatsApp o redes sociales: chantaie emocional, para intentar volver a retomar la relación; insultos v amenazas...

Sin embargo, las nuevas tecnologías. también posibilitan otras conductas de control y acoso que son normalizadas por las y los jóvenes, pero que si se analizan con "gafas violetas" son indicadores de encontrarse en una relación no saludable o "tóxica": llamadas telefónicas continuas: control sobre los contactos y amistades que se agregan a las redes sociales: prohibición de contacto real o "virtual" con algunas personas, generalmente chicos; petición de que elimine contactos o imágenes "colgadas" en redessociales: exigencia de respuesta inmediata a las conversaciones iniciadas por WhatsApp u otro canal de mensaiería instantánea: control sobre el tiempo de conexión; chantaje con dejar la relación si no consiente hacerse fotos o grabaciones de carácter sexual, argumentando que "todo el mundo lo hace" o cusándola de mojigata.

### ALGUNOS INDICADORES DE QUE VUESTRA HIJA PUEDA ENCONTRARSE EN ESTA SITUACIÓN SON:

Ha cambiado su manera de vestir y arreglarse.

Ha dejado de tener contacto con sus amig@s de siempre.

Tiene problemas para conciliar el <mark>sueño. Ha</mark> bajado su rendimiento escolar.

Muestra cambios en sus gustos y aficiones.

Ha dejado de ir a las actividades de ocio y tiempo libre.

Tiene cambios de humor repentinos sin causa aparente.

Habéis discutido por él de forma directa o indirecta.

"Notáis" que está controlada por él.

### EN ESTOS CASOS, ¿QUÉ PUEDE HACER LA FAMILIA?:

ENSEÑAR que las relaciones de pareja tienen que ser igualitarias y saludables y no "tóxicas" o que te hagan daño.

DIALOGAR sobre el amor, la sexualidad, las emociones...

CONVENCER para que cambie las contraseñas y no se las comparta; para que lo "bloquee" y/o lo "ignore".

APOYAR para que no ceda a las presiones.

AYUDAR a entender los mecanismos de control que está poniendo en marcha a través del móvil, las redes sociales,...

**DENUNCIAR la situación de ciberviolencia.** 



### PARA TERMINAR...

#### algunos recursos

www.chaval.es
www.pantallasamigas.net
www.osi.es
www.kiddia.org (Junta de Andalucía)

#### Policía Nacional

(Brigada de Investigación Tecnológica):

http://www.policia.es/colabora.php

(para denuncias y consultas):

www.policia.es/bit (web alertas tecnológicas)

Guardia Civil (Grupo de Delitos Telemáticos):

https://www.gdt.guardiacivil.es/

(para información, denuncias, consultas, etc.)

900.101.062



### **GLOSARIO**

#### Malware.

Es una aplicación informática que tiene como objetivo infiltrarse en el sistema operativo de un ordenador sin el conocimiento de su dueño/a y que puede comprometer la seguridad del mismo. Incluye virus informáticos, gusanos, troyanos y spyware (sistema espía).

### Hacking.

Es la entrada directa de una persona en un sistema informático sin el conocimiento de su dueño/a, ayudándose de alguna "vulnerabilidad" que lo permita.

#### Spam.

También llamado "correo electrónico no deseado" o "correo basura" es el conjunto de mensajes no solicitados que, enviados masivamente, están en condiciones de perjudicar el equipo informático que los reciba.

#### Actualizaciones del sistema operativo.

Son modificaciones en el sistema operativo del ordenador sugeridas por el propio fabricante con intención de solucionar problemas aparecidos o prevenir inconvenientes en el futuro. Es fundamental para la seguridad y confiabilidad del equipo.

### Fairewall (cortafuegos).

Es una aplicación informática cuya función es proteger nuestro ordenador de intrusiones externas no deseadas. Permite o limita el tráfico de información entre el ordenador y la Red.

#### Antivirus.

Es una aplicación informática diseñada para detectar, bloquear, eliminar y, si es posible, prevenir las operaciones malintencionadas (malware) en un ordenador. Es el complemento obligado de un firewall (cortafuegos).

AYUNTAMIENTO DE SEVILLA



### NOSDO

AYUNTAMIENTO DE SEVILLA

Igualdad, Juventud y Relaciones con la Comunidad Universitaria Dirección General de Igualdad y Cooperación Servicio de la mujer